Ihre Marke ist bei uns sicher

Bynders Sicherheits- und Datenschutzverpflichtung für Sie und Ihre Daten

Als weltweit eingesetzter SaaS-Anbieter befasst sich Bynder mit Gesetzen aus vielen Teilen der Welt und achtet auf die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten. Bynder basiert auf einer zuverlässigen Infrastruktur, die mehr Datenschutz, Sicherheit und sofort einsatzbereite Geschäftskontinuität bietet. Eine umfassende Informationssicherheit ist ein entscheidendes Merkmal unseres Produkts.

Unsere Zertifizierungen

- ISO 27001:2013, ISO 27018:2019 und ISO 22301:2019 zertifiziert: Jährliche unabhängige ISO-Audits von Drittanbietern für Standorte und Produkte.
- HIPAA-konform: Schutz von medizinischen Informationen und sensiblen Patientendaten.
- PCI-DSS-konform: PCI-DSS (Payment Card Industry Data Security Standard) zum Schutz von Informationen über Personen und deren Zahlungsdetails, die auf jeder Online-Plattform verwendet werden.

- GDPR- und CCPA-konform: Vollständige Übereinstimmung mit den Datenschutzgesetzen der EU, Großbritanniens und USA, einschließlich der neuesten GDPR- und CCPA-Gesetze.

Hosting-Partner AWS

Bynder hat seine Sicherheitsmaßnahmen mit Amazon Web Services (AWS) kombiniert, um sicherzustellen, dass in Bynder gespeicherte Daten vor Lecks und Sicherheitsverletzungen geschützt sind. AWS garantiert eine 99,9% Beständigkeit für alle Objektspeicher und bietet Sicherheit, die mit Ihrer Nutzung skaliert.

Technische Maßnahmen

- Öffentlich zugängliche Richtlinien. Mehr Informationen:https://www.bynder.com/de/rechtliches/datenschutzrichtlinie/
- Spezielle Sicherheitstools für das Schwachstellenmanagement, Schwachpunkte in Open Source Bibliotheken und vieles mehr.
- Jährliche Penetrationstests (basierend auf den OWASP Top 10) durch einen unabhängigen Dritten.
- Wir verschlüsseln Daten mit bewährten Algorithmen und Verschlüsselungscodes.
- Ein genau definierter SSDLC (Secure Software Delivery Lifecycle), der an den ISO-Standards ausgerichtet ist, sodass nur sichere und zuverlässige Software freigegeben wird.
- Produktinterne Funktionen wie u.a. Waiting Room, Berechtigungs- und Zugriffsrechte sowie SSO/MFA-Funktionen erfordern eine zusätzliche Sicherheitsstufe für Bynder-Benutzer und -Administratoren.

Organisatorische Maßnahmen

Das Informationssicherheitsteam von Bynder wird von unserem CISO geleitet und besteht aus geschulten Sicherheitsbeauftragten und ethischen Hackern, die die Sicherheit von Bynder-Produkten täglich überprüfen.

Die Teams von Bynder werden regelmäßig geschult und über alle Sicherheitsmaßnahmen informiert, um sicherzustellen, dass die Informationssicherheit in der kollektiven Verantwortung des Managements und der Mitarbeiter liegt.

Bynder wird mindestens einmal jährlich von einem unabhängigen Dritten überprüft, damit das Informationssicherheit-Managementsystem (ISMS) und das Business Continuity Management-System (BCMS) auf dem neuesten Stand sind und korrekt angewendet werden.

Erfahren Sie mehr über die Sicherheitsmaßnahmen, die Bynder ergreift, um die Vertraulichkeit, Integrität, Verfügbarkeit und Kontinuität von Kundendaten zu verwalten: https://www.bynder.com/de/sicherheit/